Adobe Provider Data Processing Agreement: Information Security and Privacy Terms

Effective as of April 22, 2021. These Terms replace and supersede all prior versions.

Adobe and Service Provider (the contracting entity as defined in the Agreement) have entered into an Agreement (the "Agreement") pursuant to the terms of which Service Provider may Process or store certain Adobe Information (as defined below) in connection with the services. This document describes the specific data transfer and processing requirements (including without limitation, the security and privacy requirements) applicable to Service Provider's Processing or storing of Adobe Information ("Security and Privacy Procedures"). Unless specifically defined in this document, capitalized terms shall have the meanings set forth in the Agreement.

1. **Definitions.**
   - **1.1 "Adobe's Corporate Identity Provider"** means integrating with Okta as an Identity Provider (IdP) using the SAML 2.0 protocol for any user having an '@adobe.com' e-mail address (or successor technology approved by Adobe).
   - **1.2 "Adobe Customer"** means a person who either independently or on behalf of a business entity is a customer of Adobe and/or an Adobe affiliate (e.g., Magento, Marketo).
   - **1.3 "Adobe Information"** means any Adobe or Adobe Customer Confidential Information, Cardholder Information, Personal Information, or Sensitive Personal Information (including any information derived or inferred from such Adobe Information) that is Processed or stored by Service Provider or Service Provider Parties in connection with the services. In addition to Personal Information from Adobe Customers, Adobe Information may also include Personal Information from prospects, business partners, vendors, contractors, employees, agents and advisors.
   - **1.4 "Adobe Password Standards"** means the following minimum password requirements: (i) unique user identification; (ii) minimum 12-character password; (iii) includes at least one uppercase character, one lowercase character, one digit, and one special character; (iv) must be updated every 90 days; (v) access attempts limited to six within a five-minute period; and (vi) salted and hashed.
   - **1.5 "Adobe Security Contact"** means the individual on the Adobe Information Security team that can be reached by email at noc@adobe.com or by phone at 1-800-285-1203 in the event of a Security Incident.
   - **1.6 "Cardholder Information"** means: (i) with respect to a payment card, the account holder's name, account number, service code, card validation code/value/number, PIN or PIN block, valid to and from dates and magnetic stripe data; and (ii) information relating to a payment card transaction.
   - **1.7 "Confidential Information"** refers to that information defined as Confidential in the Agreement.
   - **1.8 "Controller"** refers to the term as defined in applicable Data Protection Requirements, including without limitation, the General Data Protection Regulation (Regulation (EU) 2016/679) and the Virginia Consumer Data Protection Act (2021).
   - **1.9 "Data Protection Requirements**" means, collectively, any applicable international, national, state and local laws or regulations relating to the Processing, storage, and protection of Adobe Information.
   - **1.10 "Online Security Assessment"** means Adobe's Vendor Security Review, an online security risk assessment (or equivalent) for evaluation Service Provider's security controls.
   - **1.11 "Personal Information"** means any information that reasonably identifies or can be used to identify an individual directly or indirectly and includes 'personal data' and "sensitive personal information or data' as defined under applicable Data Protection Requirements. Personal Information may relate to any individual, such as a customer, employee, vendor, or contractor.
   - **1.12 "Processed" or "Processing"** means any operation or set of operations performed upon the Adobe Information or sets of Adobe Information, whether or not by automated means, such as access, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation,

use, transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.13 **"Processor"** refers to the term as defined in applicable Data Protection Requirements, including without limitation the General Data Protection Regulation (Regulation (EU) 2016/679) and the Virginia Consumer Data Protection Act (2021). "Processor" shall also include "Service Provider" as defined under the California Consumer Privacy Act (2018), as amended, where the processing activity relates to California consumers and Service Provider is processing Adobe Information on Adobe's behalf.

1.14 **"PCI Standards"** means the security standards for the protection of payment card data with which the payment card companies require merchants to comply, including the Payment Card Industry Security Standards currently in effect and as may be updated from time to time.

1.15 **"Public Network"** means any data network established and operated that provides data transmission services for public use, such as the Internet.

1.16 **"Secure FTP"** means "Secure File Transfer Protocol" which is a method used to encrypt and decrypt data that is transferred between a client and server, or a successor technology approved in writing by Adobe.

1.17 **"Security Incident"** means that Service Provider reasonably believes that: a) there is a substantial likelihood of accidental or unauthorized acquisition, destruction, loss, modification, use, or disclosure of, or access to, Adobe Information Processed or stored by, or on behalf of, Service Provider; or malware was or is present on a Service Provider system in a manner that Adobe users were exposed to the malware (for example, malware was present on a Service Provider system from which end users download content).

1.18 **"Service Provider Parties"** means any Service Provider employee, contractor or third party entity that Service Provider uses to provide services to Adobe under the Agreement.

1.19 **"Sensitive Personal Information"** means an individual's: (i) social security number, national identification number or equivalent, taxpayer identification number, passport number, driver's license number or other government –issued identification number; (ii) financial account number, with or without any code or password that would permit access to the account (such as bank account numbers and debit or credit card numbers); (iii) ethnicity or race information, religious, political or philosophical belief information, medical or health information, trade union membership information, details of criminal convictions or changes, biometric or genetic information (for purpose of uniquely identifying a natural person), background check information, sex life information (including sexual orientation); (iv) Cardholder Information; (v) any Personal Information defined as "Sensitive" or (equivalent) under an applicable Data Protection Requirement.

1.20 **"Strong Authentication"** means multi- factor authentication (e.g. something you know + something you have).

2. Information Security Program: Technical and Organizational Measures.

2.1 In General. Service Provider must:

a. Develop, implement, maintain, and monitor a comprehensive, written information security program that contains appropriate administrative, technical, and physical safeguards to protect against anticipated threats or hazards to the security, confidentiality, availability, or integrity of Adobe Information, including the unauthorized or accidental acquisition, disclosure, destruction, loss, alteration or use of, and the unauthorized access to, Adobe Information;

b. Conduct routine risk assessments to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, availability, and integrity of electronic, paper, and other systems Processing Adobe Information and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks;

c. Ensure that its information security program is consistent with: (i) these Security and Privacy Procedures; (ii) the Data Protection Requirements; and (iii) the PCI Standards, if Service Provider has access to or otherwise Processes or stores Cardholder Data;

d. If Service Provider Processes or stores Adobe Information in any way, it shall ensure Adobe employees or Adobe administrators with access to Adobe Information are authenticated as follows: (i) Adobe users are authenticated using either Adobe's Corporate Identity Provider or Adobe Password Standards; and (ii) all other users are authenticated via Strong Authentication or Adobe Password Standards.

e. Provide reasonable assistance to Adobe in Adobe's assessment and implementation of appropriate technical and organizational measures to ensure an appropriate level of security of Adobe Information.

f. If Service Provider transmits Adobe Information through a Public Network, Service Provider will protect it using AES-128 or equivalent encryption as defined by the most recent NIST standard, commonly implemented through protocols such as TLS, IPsec, or Secure FTP;

g. If Service Provider controls end user access to Adobe's network or systems, Service Provider (i) will implement industry-standard measures, including internet address protocol (IP) blocking technology, to prevent access to Adobe networks, systems, or information by users in embargoed countries (as identified in Country Group E:1 in Supplement No. 1 to Part 740 of the Export Administration Regulations (15 CFR Parts 730-774) or equivalent rules in the European Union and other jurisdictions in which Adobe and its affiliates operate).; and (ii) will notify the Adobe Security Contact immediately by email when it has reasonable "knowledge: (as defined in the Definitions of Terms in Part 772 of the Export Administration Regulations (15 CFR Parts 730-774) of any potential or actual activity involving access by users in Embargoed Countries to Adobe networks, systems, or information.

2.2 Service Provider Review of the Information Security Program. Service Provider reviews and updates its information security program policies at least annually or whenever there is a material change in Service Provider's practices that may reasonably affect the security, confidentiality, availability, or integrity of Adobe Information. Service Provider may not alter or modify its information security program in such a way that will weaken or compromise the security of Adobe Information. If available, Service Provider will provide to Adobe (upon request) copies of its audited security assertions (SSAE16-SOC 2 Type 2 report, or, for Service Providers outside the United States, an ISO 27001 certificate, or international equivalent) on an annual basis.

2.3 Maintaining the Information Security Program. Service Provider maintains, trains its workforce, and enforces its information security program at each location from which Service Provider provides the services. Service Provider regularly conducts network vulnerability scans, penetration testing, and incident response table top exercises as part of its information security program. Service Provider's information security program covers all networks, systems, servers, computers, notebooks, laptops, PDAs, mobile phones, and any other devices or media that Process or stores Adobe Information or that provide access to Adobe networks or systems. Service Provider's information security program includes industry standard password protections that are equivalent to the Adobe Password Standards as appropriate, firewalls, and anti-virus and malware protections to protect Adobe Information stored on computer systems. Service provider has baseline security configurations or hardening images for firewalls, routers, servers, personal computers, wireless and remote access points.

2.4 Logging Requirement. Service Provider will automatically collect system, application, and user level logs on an ongoing basis. Logs must (at a minimum) contain user name, location, date and time of access, IP address, and actions performed. Logs must be kept for a minimum of ninety (90) days and made available to Adobe for review within twenty-four (24) hours upon Adobe's request (in the event of a Security Incident) or within seventy-two (72) hours for all other requests unless otherwise agreed to in writing by Adobe. Service Provider must perform audit log collection and aggregation of all key web

service systems and applications that are involved in the Processing or storage of Adobe Information and monitor those logs for evidence of any Security Incident. Authentic Copies of Adobe Information that has been accessed or acquired by an unauthorized person must be provided promptly to Adobe Security Contact upon request.

2.5 Adobe Security Assessments. Adobe may require Service Provider to complete periodic Online Security Assessments of Service Provider's computing systems, environments, and networks involved in the Processing or storage of Adobe Information. Service Provider agrees that should the Online Security Assessment reveal a material issue in Service Provider's security or privacy controls, Adobe may suspend Service Provider's access to Adobe's computing systems and networks until such the relevant security or privacy control has been appropriately addressed. Such suspension will not be considered a material breach of the Agreement.

2.6 Magento Security, Privacy and Architecture. To the extent Service Provider will provide services that could be integrated with or accessible from any version or type of Magento platform, server or instance (including any on-premise, cloud or open source instance of Magento), Service Provider will ensure that it maintains an equivalent or greater level of security and data protection for its systems, tools, interfaces, extensions, consoles and networks consistent with Magento's Security Privacy and Architecture Guide (https://magento.com/sites/default/files/magento-security-privacy-and-architecture-guide.pdf) as may be amended from time to time. Service Provider represents and warrants that it is not aware of any defect or vulnerability that could compromise the security of any Magento system, network or platform when integrated or connected with the services.

2.7 Marketo Security, Privacy and Architecture. To the extent Service Provider will provide services that could be integrated with or accessible from any version or type of Marketo platform, server or instance (including any on-premise, cloud or open source instance of Marketo), Service Provider will ensure that it maintains an equivalent or greater level of security and data protection for its systems, tools, interfaces, extensions, consoles and networks consistent with Marketo's Technical and Organizational Measures for Data Protection (attached herein) as may be amended from time to time. Service Provider represents and warrants that it is not aware of any defect or vulnerability that could compromise the security of any Marketo system, network or platform when integrated or connected with the services.

3. Processing, Disclosure, and Destruction of Adobe Information.

3.1 Processing. In accordance with all Data Protection Requirements, Service Provider is a Processor or sub-processor Processing or storing Adobe Information on Adobe's behalf. Service Provider will ensure that the Processing and storage of Adobe Information are carried out in compliance with Adobe's instructions.

3.2 Processing of Adobe Information.

a. Scope of Processing. If applicable, the description of the Processing carried out by Service Provider is set out in the Agreement, the Online Security Assessment, and/or Addendum 1. Addendum 1 shall be populated by the parties where such information is required to be set out in these Security & Privacy Terms under Data Protection Requirements.

b. Purpose of Processing. The purpose of the Processing or storage of Adobe Information is Service Provider's provision of the services described in the Agreement.

c. Processing Limitation. Service Provider may only Process Adobe Information (i) on Adobe's behalf; (ii) in accordance with Adobe's written instructions (which include the Agreement and these Security and Privacy Procedures); and (iii) for the sole purpose of providing, operating, managing, testing, maintaining and enhancing the services and/or protecting the services from a threat to the services or Personal Information. Service Provider is not permitted to sell Adobe Information or cause, allow, or facilitate the sale of Adobe Information. Except as necessary to provide the services, Service Provider is not permitted to collect, retain, use, or disclose Adobe Information for its own purposes or for the purpose of any third party, firm, or enterprise (including affiliates). If Service Provider must

Process Personal Information for any purpose required under a Data Protection Requirement to which it is subject, Service Provider will inform Adobe of such a requirement prior to Processing the data unless prohibited by law.

d. Record of Processing Activities. Service Provider and, where applicable, Service Provider Parties will maintain a written record of its Processing activities (including in electronic form) for Personal Information and Sensitive Personal Information carried out in connection with the services. Such record will include:

i. Name and contact details of the Processor or Processors and of each Controller (as defined by the GDPR) on behalf of which the Service Provider is acting, and where applicable, of the Controller or processor's representative, and the data protection officer;

ii. the categories of Processing carried out on Adobe's behalf;

iii. where applicable, transfers of Personal Information to a third country or an international organization, including the identification of that third country or international organization, and the documentation of appropriate safeguards;

iv. where possible, a general description of the technical and organizational security measures.

e. Assistance. In accordance with the Data Protection Requirements, Service Provider shall take all reasonable steps to assist Adobe in meeting Adobe's obligations under the Data Protection Regulations (including without limitation Articles 32 to 36 of GDPR) taking into account the nature of the Processing under this Agreement.

3.3 Disclosure of Adobe Information.

a. In General. Except as may be permitted pursuant to this Section 3.3, Service Provider may not disclose Adobe Information to any third party, firm, or enterprise (including an affiliate) in violation of the terms and conditions of the Agreement or this document;

b. Subprocessors. Service Provider may use Service Provider Parties in connection with the services subject to the following requirements:

i. Service Provider must obtain Adobe's prior written approval before disclosing Personal Information to any third party (including Service Provider Parties, but specifically excluding Service Provider's employees) or, prior to disclosure or provide Adobe with a current list of Service Provider Parties (excluding Service Provider employees). The list must include the Service Provider Parties' country of location and instructions for communicating to Adobe any updates to this list.

ii. If Service Provider opts to provide Adobe with a list of Service Provider Parties (excluding Service Provider's employees), and Adobe has a reasonable basis to object to a new Service Provider Party, Adobe must promptly contact Service Provider in writing within 15 business days after receipt of such change. Adobe and Service Provider will work together without unreasonable delay to recommend an alternative arrangement. If a mutually acceptable and reasonable alternative arrangement is not found, Adobe may terminate the services without penalty.

iii. Before disclosing any Adobe Information, Service Provider must enter into a written agreement with the recipient of Adobe Information that is at least as protective as these Security and Privacy Procedures.

iv. Service Provider is at all times accountable and responsible for all actions by Service Provider Parties with respect to the disclosed Adobe Information.

c. Response to Inquiries. Service Provider must: (i) unless prohibited by law, notify Adobe immediately if Service Provider receives an inquiry or complaint from any individual, entity, organization, law enforcement, regulatory or governmental official or court authority related to or in connection with Adobe Information; (ii) following prior consultation with Adobe and having obtained Adobe's consent, respond to any inquiry from law enforcement, a government official or

court authority related to or in connection with Adobe Information within the time required by such official or authority; and (iii) provide reasonable support to Adobe in responding to such request in connection with Adobe Information. Unless prohibited by law or court order, Service Provider will notify Adobe of any anticipated disclosure to a third party. Such notification must provide Adobe with at least two (2) weeks' notice, so that Adobe or an Adobe Customer for whom Adobe processes Personal Information may, at its own expense, exercise such rights as it may have under law to prevent or limit such disclosure. Service Provider will exercise commercially reasonable efforts to prevent and limit any such disclosure and to preserve the confidentiality of the Adobe Information, including cooperating with Adobe to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to the Adobe Information.

3.4 Destruction of Adobe Information.

a. In General. If Adobe is not capable of removing or deleting Adobe Information from the services, Service Provider will, at Adobe's request or upon the expiration or termination of this Agreement for any reason, promptly return to Adobe or destroy (and certify in writing to Adobe the destruction method used, the date of destruction and the party that performed the destruction), at Adobe's option, the Adobe Information that is in Service Provider's or Service Provider Parties' possession or control. If Adobe elects to have such information returned, Service Provider will return all such information via a bonded courier. Service Provider will destroy Adobe Information stored as a backup in accordance with its written policies and normal course of operations. If Service Provider does not have a written policy for destruction of backups, Service Provider will destroy Adobe Information stored in backup or archived form as mutually agreed between the parties.

b. Disposal Methods. If Service Provider disposes of any paper, electronic, or other record containing Adobe Information, Service Provider will take all reasonable steps (based on the sensitivity of the Adobe Information) to destroy the Adobe Information by: (i) shredding; (ii) permanently erasing and deleting; (iii) degaussing; or (iv) otherwise modifying the Adobe Information in such records to make it unreadable and indecipherable. All Sensitive Personal Information must be disposed of in a manner described in (i) through (iii).

4. Cardholder Information. This section 4 is only applicable if Service Provider will Process or store Cardholder Information.

4.1 In General. If Service Provider has access to (or is permitted access to) Cardholder Information, Service Provider: (i) represents that its information security program addresses the requirements of the PCI Standards; (ii) maintains a complete audit trail of all transactions and activities associated with Cardholder Information; and (iii) does not store card validation codes/values/numbers, complete magnetic stripe data or PINs and PIN blocks.

4.2 PCI Certification. If Service Provider has access to Cardholder Information, Service Provider represents and warrants that it maintains certification of its compliance with the PCI Standards and that it regularly participates in independent, third-party monthly system vulnerability scans. Service Provider will promptly provide, at the request of Adobe, current certification of compliance with the PCI Standards, by an authority recognized by the Payment Card Industry for that purpose.

5. Personnel Security

5.1 Confidentiality. Service Provider will ensure Service Provider Parties with access to Adobe Information or who otherwise Process or store Adobe Information, are informed of the confidentiality requirements and have executed confidentiality agreements or have confidentiality obligations equivalent to the requirements of these Security and Privacy Procedures.

5.2 Training. Service Provider Parties with access to or who otherwise Process or store Adobe Information have received appropriate training regarding information security and data privacy.

5.3 Criminal History. Service Provider will not provide access to Adobe Information to any person who, to the best of Service Provider's knowledge, has been convicted of a crime (including, without limitation, any felony or misdemeanor) involving fraud or dishonesty in the past two years.

6. Physical and Environmental Security. Service Provider's information processing facilities that Process and store Adobe Information in any format (including Adobe Information maintained in paper or digital form) are housed in secure facilities and protected by perimeter security, such as barrier access controls that provide a physically secure environment from unauthorized access, damage, and interference.

7. Access Control.

7.1 In General. Service Provider has established and enforces written procedures that follow role based access control principles to control the access to systems, networks, services, and facilities that may Process or store Adobe Information. Service Provider will make such procedures available to Adobe upon request.

7.2 Access to Adobe Information. Service Provider will limit access to Adobe Information to the minimum number of Service Provider Parties who require such access in order to provide the services. Access to Adobe Information must be logged and maintained for minimum ninety (90) days and made available to Adobe upon request.

7.3 Access to Adobe Network or Systems. If Service Provider connects to Adobe's computing systems or networks, Service Provider agrees that: (i) Service Provider will not access, and will not permit any other person or entity to access, Adobe's computing systems or networks without Adobe's authorization and any such actual or attempted access will be consistent with any such authorization; and (ii) all Service Provider connectivity to Adobe's computing systems and networks and all attempt at same will be only through Adobe's security gateways/firewalls and only for the purposes of providing the services.

8. Communications and Operational Management.

8.1 In General. Service Provider monitors and manages each of its information Processing facilities, including, without limitation, implementing operational procedures, change management and incident response procedures, to ensure compliance with its obligations hereunder. Service Provider performs regular security and vulnerability scans no less frequently than monthly and remediate significant vulnerabilities as soon as possible, but within 30 days of discovery (or as mutually agreed in writing between the parties).

8.2 Anti-Malware Requirements. Service Provider has implemented anti-malware software on all systems that Process or store Adobe Information to ensure that all Adobe Information is free of malware (such as viruses, Trojan horses, worms, etc.), including laptops and other devices that Process or store Adobe Information. For services that allow an end user to upload Adobe Information that is subsequently made available for download by an end user, Service Provider will scan the information for malware prior to making it available for download.

8.3 Encryption. Service Provider will encrypt all Adobe Information, using industry standard encryption tools (or better), that Service Provider: (i) transmits or receives wirelessly or across Public Networks; (ii) stores on laptops; (iii) stores on storage media (e.g. servers, databases, backup tapes); (iv) stores on portable devices (such as USB drives, mobile and tablet devices); and (v) Processes or stores on any device that is transported outside of the physical or logical controls of Service Provider including, any printer, copier, scanner, or fax machine. Service Provider will safeguard the security and confidentiality of all encryption keys.

8.4 Data Recovery. Service Provider has deployed and tested back-up facilities to ensure that Adobe Information may be recovered in the event of a disaster or media failure.

8.5 Email Notifications. If Service Provider originates email notifications to its users, Service Provider's domain must be compliant with Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM)

protocols before January 1, 2017, or at the start of services. Service Provider is responsible for its email hygiene and Adobe shall not entertain whitelist requests. If Service Provider originates emails on behalf of Adobe (i.e., from an "…@adobe.com" email address), Service Provider must be compliant with the Domain-based Message Authentication, Reporting and Conformance (DMARC) protocol before June 1, 2017, or at the start of services.

9. Security Incidents.

9.1 In General. Service Provider is responsible for managing Security Incidents involving Adobe Information that is Processed or stored by, or on behalf of, Service Provider or Service Provider Parties. Service Provider will notify the Adobe Security Contact by email and by phone of any potential or actual Security Incidents (i) involving Personal Information within twenty four (24) hours of the occurrence; or (ii) involving all other Adobe Information within seventy two (72) hours of the occurrence. Service Provider will investigate the Security Incident, and take all necessary steps to eliminate or contain the exposures that led to such Security Incident. Service Provider must provide Adobe with a written status update, via email, within seven (7) calendar days of the occurrence of any Security Incident, detailing mitigation steps taken by Service Provider in response to such occurrence and a final report detailing the investigation and remediation within 10 business days from the close of the Security Incident (or as mutually agreed in writing between the parties).

9.2 Service Provider Cooperation. Service Provider agrees to provide (at Service Provider's sole cost) reasonable assistance and cooperation requested by Adobe, in furtherance of any correction, remediation, or investigation of a Security Incident and/or mitigation of any damage, including any notification and/or credit reporting service that Adobe may determine appropriate to send to individuals impacted or potentially impacted by such Security Incident. Unless required by law, Service Provider will not notify any individual or any third party (including any national data protection authority or equivalent regulatory body) other than law enforcement of any potential Security Incident without first consulting with and obtaining the permission of Adobe.

10. Right to Audit; Regulatory Requests; and Reasonable Assistance.

10.1 Audits.

a. Service Provider will audit the security of the computers and computing environments that it uses in Processing Personal Information for the services and the physical data centers from which Service Provider provides the services. This audit (i) will be performed at least annually; (ii) will be performed by a third party security professional (qualified auditor) at Service Provider's selection and expertise; (iii) will result in the generation of an audit report ("Audit Report") which will be Service Provider's Confidential Information; and (iv) may be performed for other purposes in addition to satisfying this requirement (as part of a regular internal security procedure).

b. Upon Adobe's written request (and no more than once per year), Service Provider will provide Adobe with a confidential summary of the most recent Audit Report with respect to Service Provider's commitments in these Security and Privacy Procedures ("Summary Report") so that Adobe may reasonably verify Service Provider's compliance with these Security and Privacy Procedures. The Summary Report is Adobe Confidential Information.

10.2 Regulatory Requests. The parties acknowledge that under certain circumstances, in order for Adobe to remain in compliance with Data Protection Requirements, it may be legally required for Adobe to verify or certify Service Provider's compliance with its obligations under these Security and Privacy Procedures by means other than reviewing the Summary Report. These means may include receiving additional information, briefings on specific security issues, or visiting premises of our Service Provider or Service Provider Parties. To the extent necessary for Adobe to ensure compliance with applicable Data Protection Requirement, the parties agree to the following process:

a. Service Provider will submit a request for additional information in writing to the Service Provider Party(ies) specifying such details as may be needed to enable Service Provider Party(ies) to review the request. The request will include information such as the information being requested, in what form the response(s) is needed, and the underlying regulatory requirement for the request ("Regulatory Request").

b. Within a reasonable time after Service Provider has received and reviewed the Regulatory Request, Service Provider, Service Provider Party(ies) and Adobe will discuss and work in good faith towards agreeing on a plan ("Compliance Review Plan") to determine the details of how the Regulatory Request can be addressed. A timeframe for reviewing the Regulatory Request and preparing the Compliance Review Plan will be agreed between the parties, taking into account Data Protection Requirements and the urgency of the matter. If Service Provider or Service Provider Party(ies) believe that it is not possible to meet a specific time frame set by the Data Protection Authority in connection with the Regulatory Request, Service Provider and/or Service Provider Party(ies) will provide Adobe with reasonable assistance to provide the Data Protection Authority with the details for why the timeframes cannot be reasonably met. The parties agree to use the least intrusive means for the Service Provider Party(ies) to verify its compliance with its obligations under this Section taking into account the Data Protection Requirements and the urgency of the Regulatory Request and potential impact to Service Provider and Service Provider Party(ies) business operations and confidentiality of other customers information.

c. Any information, responses and documentation provided by Service Provider, Service Provider Party(ies) or their respective auditors in relation to this section will be treated by Adobe and its auditors as Confidential Information of Service Provider.

d. Assistance under this Section 10.2 shall be at Adobe's sole expense, except where such investigation was required due to Service Provider's (including Service Provider Parties) acts or omissions, in which case such assistance shall be at Service Provider's sole expense.

10.3 Impact of Audit Requirements on Standard Contractual Clauses. In the event Standard Contractual Clauses are applicable, nothing in this Section 10 varies, modifies, or affects any supervisory authority's or individual's rights under the Standard Contractual Clauses.

10.4 Reasonable Assistance: Correction, deletion, and blocking of data. To the extent Adobe does not have the ability to access Personal Information to respond to requests from individuals enforcing their right to correct, amend, port, or delete their data upon request (as permitted by Data Protection Requirements), Service Provider will assist Adobe with any reasonable request to do so within 7 business days of Adobe's request. If an individual should communicate directly with the Service Provider to request enforcement of their individual rights under Data Protection Requirements in connection with the services provided to Adobe by Service Provider, Service Provider will promptly notify Adobe of the request and will provide Adobe with reasonable assistance in processing any such request.

11. International Data Transfers and Processing of Personal Information.

11.1 Transfer of European Personal Information. If Service Provider accesses or Processes any Personal Information that is subject to the General Data Protection Regulation (Regulation (EU) 2016/679) and/or data protection laws in the United Kingdom and/or data protection laws in Switzerland, and any successors or amendement thereto ("European Personal Information"), from outside of the European Union or European Economic Area or any country deemed adequate by the European Commission (a "Third Country"), Service Provider shall only do so with Adobe's prior written consent and, where such prior written consent is granted, Service Provider will, for the duration of the Processing or storage of European Personal Information:

a. enter into the Standard Contractual Clauses for the transfer of personal data to data processors established in third countries adopted by the European Commission decision of 5 February 2010, published under document number C(2010) 593 2010/87/EU (as may be amended or replaced from

time to time by the European Commission or another method under Data Protection Requirements and as may need to be amended for the purposes of Swiss data protection law) ("SCCs") in relation to the transfer of European Personal Information with Adobe and / or Adobe's international affiliates (either as a Processor where Adobe and/or its affiliates are Controllers or as a sub-processor pursuant to and in accordance with clause 11 of the SCCs where Adobe and/or its affiliates have entered into SCCs with other Adobe EEA, UK or Swiss affiliates or Adobe customers); or

b. where Service Provider is established in the EEA and Service Provider, to the extent permitted by Section 3.3, proposes to transfer European Personal Information to a third party in a Third Country, ensure that such third party enters into the SCCs in relation to the transfer of European Personal Information directly with Adobe and / or Adobe's international affiliates (either as a Processor where Adobe and/or its affiliates are Controllers or as a sub-processor pursuant to and in accordance with clause 11 of the SCCs where Adobe and/or its affiliates have entered into SCCs with other Adobe EEA, UK or Swiss affiliates or with Adobe's customers).

The parties may agree to other mechanisms to transfer European Personal Information to Third Countries, such as mechanisms contained in GDPR (Regulation (EU) 2016/679), as approved by the European Commission or another mechanism approved under applicable Data Protection Requirements, so long as such mechanism remains lawful in accordance with the decisions of the Court of Justice of the European Union and other applicable Data Protection Requirements. Adobe may, at no cost, suspend or require Service Provider to suspend, any transfers of Personal Information which in Adobe's reasonable opinion do not comply or which cease to comply with Data Protection Requirements. In such case the parties shall negotiate in good faith a solution to enable the transfers of Personal Information to be reinstated in compliance with Data Protection Requirements. If Adobe and Service Provider (and any sub-processor, where relevant) are unable to promptly agree a solution, then Adobe shall have the right to terminate the Agreement in whole or in part by providing Service Provider written notice of termination which shall be effective as of the date of such notice of termination or such later date as determined by Adobe. The parties acknowledge and agree that a failure or a delay by Adobe to exercise its rights under this Section shall not constitute a waiver of these rights and does not prevent or restrict Adobe from exercising or further exercising its rights under this Section. No single or partial exercise of the rights under this Section shall prevent or restrict the further exercise of such rights.

11.2 All Other Transfers. If Service Provider accesses or Processes any Personal Information related to individuals outside of the EU/EEA that is subject to data transfer requirements, Service Provider will reasonably cooperate with Adobe to establish appropriate transfer mechanisms for such transfers.

11.3 Processing Personal Information. Service Provider agrees that it will only Process or store Personal Information to the extent necessary to perform its obligations under the Agreement (and not for any other purpose) and in compliance with applicable Data Protection Requirements. Service Provider shall take all appropriate legal, organizational and technical measures to comply with its obligations under this clause 113 and applicable Data Protection Requirements, in particular having regard to the nature of the Personal Information. Service Provider must promptly notify Adobe of any actual or alleged breach of its obligations under this clause 11.3 or any inquiry, request or complaint received in relation to the Personal Information, and must comply with any directions given by Adobe in relation to the Personal Information. Service Provider shall, upon request and within a reasonable time, correct, delete, or block Personal Information from further Processing. The Service Provider will only Process or store the Personal Information as instructed by Adobe and its affiliates and may disclose Personal Information only to Service Provider Parties who have a need to know and will ensure that such Service Provider Parties protect Personal Information as required by this document.

11.4 **Adobe Affiliates**. Service Provider acknowledges that the provisions of this document are intended to inure to the benefit of Adobe affiliated entities (collectively **"Adobe Affiliates"**) as third party beneficiaries of this document, and the Adobe Affiliates will be entitled to enforce such provisions against Service Provider. Service Provider further acknowledges that the Adobe Affiliates accept their third party beneficiary rights hereunder and that such rights will be deemed irrevocable. The respective rights and obligations of Service Provider under this document shall survive the termination, expiration, or other conclusion of this Agreement.

12. Miscellaneous

12.1 **Service Provider Obligations.** The obligations of Service Provider under this document shall continue for so long as Service Provider continues to Process or store Adobe Information, even if all agreements between Service Provider and Adobe have expired or been terminated.

12.2 **Indemnification.** Service Provider shall indemnify, hold harmless, and defend Adobe, its affiliates, and its and their officers, directors, employees, agents, successors, and assigns from and against any and all claims, losses, liabilities, damages, settlements, expenses and costs (including attorneys' fees and court costs) and any and all threatened claims, losses, liabilities, damages, settlements, expenses and costs arising from, in connection with, or based on allegations of, any of the following: (A) a material violation of the requirements of this document or the Data Protection Requirements; (B) a Security Incident; (C) the negligence or willful misconduct of Service Provider, Service Provider Parties or any third party to whom Service Provider provides access to Adobe Information or systems, with respect to security or confidentiality of Adobe Information; (D) remedial action taken by Adobe as the result of a Security Incident; and (E) any other costs incurred by Adobe necessary to enforce Adobe's rights in this document. Except as otherwise provided herein, Service Provider shall be fully responsible for, and shall pay, all costs and expenses incurred by Service Provider or Service Provider Parties with respect to the obligations imposed under this document.

12.3 **Inability to Perform; Material Breach.** In the event that Service Provider is unable to comply with the obligations stated in this document, Service Provider must promptly notify Adobe. Adobe may be entitled (at its option) to suspend the transfer of Adobe Information, require Service Provider to cease Processing relevant Adobe Information and/or immediately terminate the Agreement. Failure to materially comply with these Security and Privacy Procedures constitutes a material breach of the Agreement by Service Provider, entitling Adobe to the remedies provided for under the Agreement.

12.4 **Termination.** Adobe may terminate the Agreement immediately as a result of a material failure by Service Provider to comply with the requirements of this document.

12.5 **Trade Compliance.** The parties agree that each may provide the other with access to information, products, technologies, or services (hereafter referred to as "Item(s)") that may be subject to the trade control laws of the United States and other national governments regardless of where the Item is received. Each party is responsible for complying with all applicable laws that may impact each party's right to import, export, or use the Items.

ADDENDUM 1

DESCRIPTION OF PROCESSING ACTIVITIES FOR EUROPEAN PERSONAL DATA (IF APPLICABLE)

1.1 Subject Matter of the Processing	The subject matter of the Processing is the Service provided by Service Provider pursuant to the Agreement or related order forms or statements of work.
1.2 Duration of Processing	The Processing will continue until the expiration or termination of the Agreement or related Order Form unless otherwise instructed by Adobe.
1.3 Categories of Data Subjects	Adobe's EU, EEA, and UK end users, customers, prospects, business partners, vendors, contractors, employees, agents, and advisors who are natural persons and whose Personal Data is Processed as part of the Services.
1.4 Name and Purpose of Processing	The purpose of the Processing of Adobe's European Personal Data is the performance of the Services pursuant to the Agreement, Order Form, or Statement of Work.
1.5 Types/Categories of European Personal Data	**[TO BE COMPLETED BY SERVICE PROVIDER]**
1.6 Service Provider Subprocessors	**[TO BE COMPLETED BY SERVICE PROVIDER]**